CLAIM AMENDMENTS

1. (Currently Amended) A method for managing addition and deletion of network nodes from and to a secure multicast or broadcast group of network nodes in a communications network without a single point of failure, wherein each of the network nodes is associated with one of a plurality of ~~replicated~~ group controllers, wherein each group controller of the plurality of group controllers is a replica of a particular group controller, and wherein the network nodes and the plurality of group controllers are logically organized in a binary tree that represents the network nodes and the plurality of group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the secure multicast or broadcast group, intermediate nodes represent other network nodes, and root nodes represent the plurality of group controllers, the method comprising the steps of:

joining ~~one of the~~ a first group ~~controllers~~ controller to the plurality of ~~replicated~~ group controllers in a local network;

establishing~~, by one of the group controllers,~~ a secure communication channel between ~~one of~~ the first group ~~controllers~~ controller and ~~another~~ a second group controller of the plurality of group controllers using a key exchange protocol;

receiving a request to add or delete a network node of the secure multicast or broadcast group from a load balancer that is coupled to the plurality of group controllers;

creating and storing a new group session key for each network node represented in each branch of the binary tree that is affected by adding or deleting the network node from the secure multicast or broadcast group; and

distributing a group session key from ~~one of the~~ a third group ~~controllers~~ controller of the plurality of group controllers to the network nodes.

2. (Currently Amended) A method as recited in Claim 1, wherein distributing a group session key further comprises:

receiving a token value at the third group controller to designate the third group controller as having permission to selectively generate the group session key and to generate node keys associated with the intermediate nodes and the leaf nodes; and

creating and storing the group session key only when the third group controller has the token value.

3. (Currently Amended) A method as recited in Claim 1, wherein distributing a group session key further comprises:

determining whether the secure multicast or broadcast group has a network node that is leaving the secure multicast or broadcast group;

determining which of the intermediate nodes are affected by the leaving node;

updating keys associated with the affected intermediate nodes;

generating a new group session key; and

sending the new group session key to the leaf nodes.

4. (Currently Amended) A method as recited in Claim 3, wherein updating keys comprises:

generating a new key of a parent node of the leaving node; and

encrypting the new key of the parent node with a key of a network node adjacent to the parent node.

5. (Currently Amended) A method as recited in Claim 1, wherein distributing a group session key further comprises:

receiving a request message from one of the ~~plurality of~~ network nodes to join the secure multicast or broadcast group;

determining which of the intermediate nodes are affected by the joining node;

updating keys associated with the affected intermediate nodes;

generating a new group session key and a private key of the joining node; and

sending a message comprising the new group session key, the private key, and the updated keys of affected intermediate nodes to the joining node.

6. (Original) A method as recited in Claim 5, wherein updating keys comprises performing a one way hash function on the keys associated with the affected intermediate nodes.

7. (Original) A method as recited in Claim 1, wherein receiving a request comprises receiving the request at a load balancer having a single virtual address that represents the plurality of group controllers.

8. (Currently Amended) A method as recited in Claim 7, further comprising the step of load balancing network traffic that is directed from a plurality of the network nodes to the plurality of group controllers.

9. (Currently Amended) A method as recited in Claim 1, wherein establishing a secure communication channel comprises exchanging a public key of the first group controller with all other group controllers in the plurality of ~~replicated~~ group controllers based upon optimized broadcast Diffie-Hellman protocol.

10. (Currently Amended) A method as recited in Claim 5, wherein establishing a secure communication channel comprises:
receiving a public key value that is broadcast by the joining node;
sending a collective public key value from the network nodes to the joining node;
computing a shared secret key; and
creating and storing a group shared secret key by exchanging private key values.

11. (Currently Amended) A computer-readable medium comprising one or more sequences of instructions for managing addition and deletion of network nodes from and to a secure multicast or broadcast group of network nodes in a communications network without a single point of failure, wherein each of the network nodes is associated with one of a plurality of ~~replicated~~ group controllers, wherein each group controller of the plurality of group controllers is a replica of a particular group controller, and wherein the network nodes and the plurality of group controllers are logically organized in a binary tree that represents the network nodes and the plurality of group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the secure multicast or broadcast group, intermediate nodes

represent other network nodes, and root nodes represent the plurality of group controllers, and which instructions, when executed by one or more processors, cause the processors to carry out the steps of:

joining ~~one of the~~ a first group ~~controllers~~ controller to the plurality of ~~replicated~~ group controllers in a local network;

establishing~~, by one of the group controllers,~~ a secure communication channel between ~~one of~~ the first group ~~controllers~~ controller and ~~another~~ a second group controller of the plurality of group controllers using a public key exchange protocol;

receiving a request to add or delete a network node of the secure multicast or broadcast group from a load balancer that is coupled to the plurality of group controllers;

creating and storing a new group session key for each network node represented in each branch of the binary tree that is affected by adding or deleting the network node from the secure multicast or broadcast group; and

distributing a group session key from ~~one of the~~ a third group ~~controllers~~ controller of the plurality of group controllers to the network nodes.

12. (Currently Amended) A computer-readable medium as recited in Claim 11, wherein distributing a group session key further comprises:

receiving a token value at the third group controller to designate the third group controller as having permission to selectively generate the group session key and to generate node keys associated with the intermediate nodes and the leaf nodes; and

creating and storing the group session key only when the third group controller has the token value.

13. (Currently Amended) A computer-readable medium as recited in Claim 11, wherein distributing a group session key further comprises:

determining whether the secure multicast or broadcast group has a network node that is leaving the secure multicast or broadcast group;

determining which of the intermediate nodes are affected by the leaving node;

updating keys associated with the affected intermediate nodes;

generating a new group session key; and
sending the new group session key to the leaf nodes.

14. (Currently Amended) A computer-readable medium as recited in Claim 3, wherein updating keys comprises:
generating a new key of a parent node of the leaving node; and
encrypting the new key of the parent node with a key of a network node adjacent to the parent node.

15. (Currently Amended) A computer-readable medium as recited in Claim 11, wherein distributing a group session key further comprises:
receiving a request message from one of the ~~plurality of~~ network nodes to join the secure multicast or broadcast group;
determining which of the intermediate nodes are affected by the joining node;
updating keys associated with the affected intermediate nodes;
generating a new group session key and a private key of the joining node; and
sending a message comprising the new group session key, the private key, and the updated keys of affected intermediate nodes to the joining node.

16. (Original) A computer-readable medium as recited in Claim 15, wherein updating keys comprises performing a one way hash function on the keys associated with the affected intermediate nodes.

17. (Original) A computer-readable medium as recited in Claim 11, wherein receiving a request comprises receiving the request at a load balancer having a single virtual address that represents the plurality of group controllers.

18. (Currently Amended) A computer-readable medium as recited in Claim 17, further comprising instructions which, when executed by the one or more processors, cause the processors to carry out the step of load balancing network traffic that is directed from a plurality of the network nodes to the plurality of group controllers.

19. (Currently Amended) A computer-readable medium as recited in Claim 11, wherein establishing a secure communication channel comprises exchanging a public key of the first group controller with all other group controllers in the plurality of ~~replicated~~ group controllers based upon Diffie-Hellman protocol.

20. (Currently Amended) A computer-readable medium as recited in Claim 15, wherein establishing a secure communication channel comprises:
receiving a public key value that is broadcast by the joining node;
sending a collective public key value from the network nodes to the joining node;
computing a shared secret key; and
creating and storing a group shared secret key by exchanging private key values.

21. (Currently Amended) A method of managing addition and deletion of network nodes from and to a secure multicast or broadcast group of network nodes in a communications network, wherein each of the network nodes is associated with a first group controller comprising information that is replicated in a plurality of group controllers, and wherein the network nodes and the plurality of group controllers are logically organized in a binary tree that represents the network nodes and the plurality of group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the secure multicast or broadcast group, intermediate nodes represent other network nodes, and root nodes represent the plurality of group controllers, the method comprising the steps of:
joining the first group controller in a local network in which the plurality of group controllers are coupled;
establishing a secure channel between the first group controller and the plurality of group controllers through secure key exchange;
receiving a request to add or delete a network node from a load balancer that controls distribution of requests to the plurality of group controllers;
generating a new group session key for each network node represented in each branch of the binary tree that is affected by adding or deleting the network node from the secure multicast or broadcast group; and
distributing the group session key from the first group controller to the other group controllers of the plurality of group controllers over the secure channel.

22. (Currently Amended) A method as recited in Claim 21, further comprising the ~~steps~~ step of generating the group session key only when the first group controller is designated as a master group controller that is authorized to join network nodes and generate group session keys.

23. (Currently Amended) A method as recited in Claim 22, further comprising the ~~steps~~ step of successively designating different ~~ones~~ group controllers of the plurality of group controllers as the master group controller in real time.

24. (Currently Amended) A method for creating a secure multicast or broadcast group, the method comprising the steps of:

establishing a secure communication channel among a plurality of group controllers via a public key exchange protocol;

load balancing traffic emanating from a plurality of network nodes to the plurality of group controllers; and

distributing a group session key by one of the group controllers based upon a logical arrangement of the network nodes in a binary tree structure, the binary tree structure having a root node, intermediate nodes, and leaf nodes, wherein the plurality of network nodes correspond to leaf nodes of the binary tree structure and the plurality of group controllers correspond to the root node.

25. (Original) The method as recited in Claim 24, wherein the step of distributing further comprises:

circulating a token among the plurality of group controllers to designate the one group controller as having permission to selectively generate the group session key and keys associated with the intermediate nodes and the leaf nodes; and

selectively generating the group session key based upon the circulating step.

26. (Currently Amended) The method as recited in Claim 24, wherein the step of distributing further comprises:

detecting whether the secure multicast or broadcast group has a network node that is leaving the secure multicast or broadcast group;

determining which of the intermediate nodes are affected in response to the detecting step;

updating keys associated with the affected intermediate nodes;

generating a new group session key; and

sending the new group session key to the leaf nodes.

27. (Currently Amended) The method as recited in Claim 26, wherein the step of updating comprises:

generating a new key of a parent node of the leaving node; and

encrypting the new key of the parent node with a key of a network node adjacent to the parent node.

28. (Currently Amended) The method as recited in Claim 24, wherein the step of distributing further comprises:

receiving a request message from one of the plurality of network nodes to join the secure multicast or broadcast group;

determining which of the intermediate nodes are affected in response to the receiving step;

updating keys associated with the affected intermediate nodes;

generating a new group session key and a private key of the joining node; and

sending a message comprising the new group session key, the private key, and the updated keys of affected intermediate nodes to the joining node.

29. (Original) The method as recited in Claim 28, wherein the step of updating comprises performing a one way hash function on the keys associated with the affected intermediate nodes.

30. (Original) The method as recited in Claim 24, further comprising addressing the plurality of group controllers using a single virtual address.

31. (Currently Amended) A computer system that can manage addition and deletion of network nodes from and to a secure multicast or broadcast group of network nodes in a communications network without a single point of failure, wherein each of the network nodes is associated with one of a plurality of ~~replicated~~ group controllers, wherein each group controller of the plurality of group controllers is a replica of a particular group controller, and wherein the network nodes and the plurality of group controllers are logically organized in a binary tree that represents the network nodes and the plurality of group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the secure multicast or broadcast group, intermediate nodes represent other network nodes, and root nodes represent the plurality of group controllers, the computer system comprising:

a load balancer coupled to the plurality of group controllers for interfacing inbound service requests to a selected ~~one~~ group controller of the plurality of group controllers;

a bus coupled to the load balancer for transferring data;

one or more processors coupled to the bus for selectively generating a group session key under control of program instructions;

a memory coupled to the one or more processors via the bus;

one or more sequences of program instructions stored in the memory which, when executed by the one or more processors cause the one or more processors to perform the steps of:

joining ~~one of the~~ a first group ~~controllers~~ controller to the plurality of ~~replicated~~ group controllers in a local network;

establishing~~, by one of the group controllers,~~ a secure communication channel between ~~one of~~ the first group ~~controllers~~ controller and ~~another~~ a second group controller of the plurality of group controllers using a key exchange protocol;

receiving a request to add or delete a network node of the secure multicast or broadcast group from [[a]] the load balancer that is coupled to the plurality of group controllers;

creating and storing a new group session key for each network node represented in each branch of the binary tree that is affected by adding or deleting the network node from the secure multicast or broadcast group;

distributing [[a]] the group session key from ~~one of the~~ a third group ~~controllers~~ controller of the plurality of group controllers to the network nodes.

32. (New) A computer system as recited in Claim 31, wherein distributing a group session key further comprises:

receiving a token value at the third group controller to designate the third group controller as having permission to selectively generate the group session key and to generate node keys associated with the intermediate nodes and the leaf nodes; and

creating and storing the group session key only when the third group controller has the token value.

33. (New) A computer system as recited in Claim 31, wherein distributing a group session key further comprises:

determining whether the secure multicast or broadcast group has a network node that is leaving the secure multicast or broadcast group;

determining which of the intermediate nodes are affected by the leaving node;

updating keys associated with the affected intermediate nodes;

generating a new group session key; and

sending the new group session key to the leaf nodes.

34. (New) A computer system as recited in Claim 33, wherein updating keys comprises:

generating a new key of a parent node of the leaving node; and

encrypting the new key of the parent node with a key of a network node adjacent to the parent node.

35. (New) A computer system as recited in Claim 31, wherein distributing a group session key further comprises:
receiving a request message from one of the network nodes to join the secure multicast or broadcast group;
determining which of the intermediate nodes are affected by the joining node;
updating keys associated with the affected intermediate nodes;
generating a new group session key and a private key of the joining node; and
sending a message comprising the new group session key, the private key, and the updated keys of affected intermediate nodes to the joining node.

36. (New) A computer system as recited in Claim 35, wherein updating keys comprises performing a one way hash function on the keys associated with the affected intermediate nodes.

37. (New) A computer system as recited in Claim 31, wherein receiving a request comprises receiving the request at a load balancer having a single virtual address that represents the plurality of group controllers.

38. (New) A computer system as recited in Claim 37, further comprising one or more sequences of program instructions stored in the memory which, when executed by the one or more processors cause the one or more processors to perform the step of load balancing network traffic that is directed from a plurality of the network nodes to the plurality of group controllers.

39. (New) A computer system as recited in Claim 31, wherein establishing a secure communication channel comprises exchanging a public key of the first group controller with all other group controllers in the plurality of group controllers based upon optimized broadcast Diffie-Hellman protocol.

40. (New) A computer system as recited in Claim 35, wherein establishing a secure communication channel comprises:
receiving a public key value that is broadcast by the joining node;
sending a collective public key value from the network nodes to the joining node;
computing a shared secret key; and

creating and storing a group shared secret key by exchanging private key values.

41. (New) An apparatus for managing addition and deletion of network nodes from and to a secure multicast or broadcast group of network nodes in a communications network without a single point of failure, wherein each of the network nodes is associated with one of a plurality of group controllers, wherein each group controller of the plurality of group controllers is a replica of a particular group controller, and wherein the network nodes and the plurality of group controllers are logically organized in a binary tree that represents the network nodes and the plurality of group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the secure multicast or broadcast group, intermediate nodes represent other network nodes, and root nodes represent the plurality of group controllers, the apparatus comprising:

means for joining a first group controller to the plurality of group controllers in a local network;

means for establishing a secure communication channel between the first group controller and a second group controller of the plurality of group controllers using a key exchange protocol;

means for receiving a request to add or delete a network node of the secure multicast or broadcast group from a load balancer that is coupled to the plurality of group controllers;

means for creating and storing a new group session key for each network node represented in each branch of the binary tree that is affected by adding or deleting the network node from the secure multicast or broadcast group; and

means for distributing a group session key from a third group controller of the plurality of group controllers to the network nodes.

42. (New) An apparatus as recited in Claim 41, wherein the means for distributing a group session key further comprises:

means for receiving a token value at the third group controller to designate the third group controller as having permission to selectively generate the group session key and to generate node keys associated with the intermediate nodes and the leaf nodes; and

means for creating and storing the group session key only when the third group controller has the token value.

43. (New) An apparatus as recited in Claim 41, wherein the means for distributing a group session key further comprises:
means for determining whether the secure multicast or broadcast group has a network node that is leaving the secure multicast or broadcast group;
means for determining which of the intermediate nodes are affected by the leaving node;
means for updating keys associated with the affected intermediate nodes;
means for generating a new group session key; and
means for sending the new group session key to the leaf nodes.

44. (New) An apparatus as recited in Claim 43, wherein the means for updating keys comprises:
means for generating a new key of a parent node of the leaving node; and
means for encrypting the new key of the parent node with a key of a network node adjacent to the parent node.

45. (New) An apparatus as recited in Claim 41, wherein the means for distributing a group session key further comprises:
means for receiving a request message from one of the network nodes to join the secure multicast or broadcast group;
means for determining which of the intermediate nodes are affected by the joining node;
means for updating keys associated with the affected intermediate nodes;
means for generating a new group session key and a private key of the joining node; and
means for sending a message comprising the new group session key, the private key, and the updated keys of affected intermediate nodes to the joining node.

46. (New) An apparatus as recited in Claim 45, wherein the means for updating keys comprises means for performing a one way hash function on the keys associated with the affected intermediate nodes.

47. (New) An apparatus as recited in Claim 41, wherein the means for receiving a request comprises means for receiving the request at a load balancer having a single virtual address that represents the plurality of group controllers.

48. (New) An apparatus as recited in Claim 47, further comprising means for load balancing network traffic that is directed from a plurality of the network nodes to the plurality of group controllers.

49. (New) An apparatus as recited in Claim 41, wherein the means for establishing a secure communication channel comprises means for exchanging a public key of the first group controller with all other group controllers in the plurality of group controllers based upon optimized broadcast Diffie-Hellman protocol.

50. (New) An apparatus as recited in Claim 45, wherein the means for establishing a secure communication channel comprises:
means for receiving a public key value that is broadcast by the joining node;
means for sending a collective public key value from the network nodes to the joining node;
means for computing a shared secret key; and
means for creating and storing a group shared secret key by exchanging private key values.

51. (New) A computer-readable medium comprising one or more sequences of instructions for managing addition and deletion of network nodes from and to a secure multicast or broadcast group of network nodes in a communications network, wherein each of the network nodes is associated with a first group controller comprising information that is replicated in a plurality of group controllers, and wherein the network nodes and the plurality of group controllers are logically organized in a binary tree that represents the network nodes and the plurality of group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the secure multicast or broadcast group, intermediate nodes represent other network nodes, and root nodes represent the plurality of group controllers, and which instructions, when executed by one or more processors, cause the processors to carry out the steps of:

joining the first group controller in a local network in which the plurality of group controllers are coupled;

establishing a secure channel between the first group controller and the plurality of group controllers through secure key exchange;

receiving a request to add or delete a network node from a load balancer that controls distribution of requests to the plurality of group controllers;

generating a new group session key for each network node represented in each branch of the binary tree that is affected by adding or deleting the network node from the secure multicast or broadcast group; and

distributing the group session key from the first group controller to the other group controllers of the plurality of group controllers over the secure channel.

52. (New) A computer-readable medium as recited in Claim 51, further comprising instructions to carry out the step of generating the group session key only when the first group controller is designated as a master group controller that is authorized to join network nodes and generate group session keys.

53. (New) A computer-readable medium as recited in Claim 52, further comprising instructions for carrying out the step of successively designating different group controllers of the plurality of group controllers as the master group controller in real time.

54. (New) A computer-readable medium comprising one or more sequences of instructions for creating a secure multicast or broadcast group, and which instructions, when executed by one or more processors, cause the processors to carry out the steps of:

establishing a secure communication channel among a plurality of group controllers via a public key exchange protocol;

load balancing traffic emanating from a plurality of network nodes to the plurality of group controllers; and

distributing a group session key by one of the group controllers based upon a logical arrangement of the network nodes in a binary tree structure, the binary tree structure having a root node, intermediate nodes, and leaf nodes, wherein the plurality of network nodes correspond to leaf nodes of the binary tree structure and the plurality of group controllers correspond to the root node.

55. (New) The computer-readable medium as recited in Claim 54, wherein the step of distributing further comprises:

circulating a token among the plurality of group controllers to designate the one group controller as having permission to selectively generate the group session key and keys associated with the intermediate nodes and the leaf nodes; and

selectively generating the group session key based upon the circulating step.

56. (New) The computer-readable medium as recited in Claim 54, wherein the step of distributing further comprises:

detecting whether the secure multicast or broadcast group has a network node that is leaving the secure multicast or broadcast group;

determining which of the intermediate nodes are affected in response to the detecting step;

updating keys associated with the affected intermediate nodes;

generating a new group session key; and
sending the new group session key to the leaf nodes.

57. (New) The computer-readable medium as recited in Claim 56, wherein the step of updating comprises:
generating a new key of a parent node of the leaving node; and
encrypting the new key of the parent node with a key of a network node adjacent to the parent node.

58. (New) The computer-readable medium as recited in Claim 54, wherein the step of distributing further comprises:
receiving a request message from one of the plurality of network nodes to join the secure multicast or broadcast group;
determining which of the intermediate nodes are affected in response to the receiving step;
updating keys associated with the affected intermediate nodes;
generating a new group session key and a private key of the joining node; and
sending a message comprising the new group session key, the private key, and the updated keys of affected intermediate nodes to the joining node.

59. (New) The computer-readable medium as recited in Claim 58, wherein the step of updating comprises performing a one way hash function on the keys associated with the affected intermediate nodes.

60. (New) The computer-readable medium as recited in Claim 54, further comprising instructions for carrying out the step of addressing the plurality of group controllers using a single virtual address.

61. (New) A computer system that can manage addition and deletion of network nodes from and to a secure multicast or broadcast group of network nodes in a communications network, wherein each of the network nodes is associated with a first group controller comprising information that is replicated in a plurality of group controllers, and wherein the network nodes and the plurality of group controllers are logically organized in a binary tree that represents the network nodes and the plurality of group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the secure multicast or broadcast group, intermediate nodes represent other network nodes, and root nodes represent the plurality of group controllers, the computer system comprising:

a load balancer coupled to the plurality of group controllers for interfacing inbound service requests to a selected group controller of the plurality of group controllers;

a bus coupled to the load balancer for transferring data;

one or more processors coupled to the bus for selectively generating a group session key under control of program instructions;

a memory coupled to the one or more processors via the bus;

one or more sequences of program instructions stored in the memory which, when executed by the one or more processors cause the one or more processors to perform the steps of:

joining the first group controller in a local network in which the plurality of group controllers are coupled;

establishing a secure channel between the first group controller and the plurality of group controllers through secure key exchange;

receiving a request to add or delete a network node from the load balancer that controls distribution of requests to the plurality of group controllers;

generating a new group session key for each network node represented in each branch of the binary tree that is affected by adding or deleting the network node from the secure multicast or broadcast group; and

distributing the group session key from the first group controller to the other group controllers of the plurality of group controllers over the secure channel.

62. (New) A computer system as recited in Claim 61, further comprising instructions to perform the step of generating the group session key only when the first group controller is designated as a master group controller that is authorized to join network nodes and generate group session keys.

63. (New) A computer system as recited in Claim 62, further comprising instructions to perform the step of successively designating different group controllers of the plurality of group controllers as the master group controller in real time.

64. (New) A computer system that can create a secure multicast or broadcast group, the computer system comprising:

a load balancer coupled to the plurality of group controllers for interfacing inbound service requests to a selected group controller of the plurality of group controllers;

a bus coupled to the load balancer for transferring data;

one or more processors coupled to the bus for selectively generating a group session key under control of program instructions;

a memory coupled to the one or more processors via the bus;

one or more sequences of program instructions stored in the memory which, when executed by the one or more processors cause the one or more processors to perform the steps of:

establishing a secure communication channel among a plurality of group controllers via a public key exchange protocol;

load balancing traffic emanating from a plurality of network nodes to the plurality of group controllers; and

distributing a group session key by one of the group controllers based upon a logical arrangement of the network nodes in a binary tree structure, the binary tree structure having a root node, intermediate nodes, and leaf nodes, wherein the plurality of network nodes correspond to leaf nodes of the binary tree structure and the plurality of group controllers correspond to the root node.

65. (New) The computer system as recited in Claim 64, wherein the step of distributing further comprises:

circulating a token among the plurality of group controllers to designate the one group controller as having permission to selectively generate the group session key and keys associated with the intermediate nodes and the leaf nodes; and

selectively generating the group session key based upon the circulating step.

66. (New) The computer system as recited in Claim 64, wherein the step of distributing further comprises:

detecting whether the secure multicast or broadcast group has a network node that is leaving the secure multicast or broadcast group;

determining which of the intermediate nodes are affected in response to the detecting step;

updating keys associated with the affected intermediate nodes;

generating a new group session key; and

sending the new group session key to the leaf nodes.

67. (New) The computer system as recited in Claim 66, wherein the step of updating comprises:

generating a new key of a parent node of the leaving node; and

encrypting the new key of the parent node with a key of a network node adjacent to the parent node.

68. (New) The computer system as recited in Claim 64, wherein the step of distributing further comprises:

receiving a request message from one of the plurality of network nodes to join the secure multicast or broadcast group;

determining which of the intermediate nodes are affected in response to the receiving step;

updating keys associated with the affected intermediate nodes;

generating a new group session key and a private key of the joining node; and

sending a message comprising the new group session key, the private key, and the updated keys of affected intermediate nodes to the joining node.

69. (New) The computer system as recited in Claim 68, wherein the step of updating comprises performing a one way hash function on the keys associated with the affected intermediate nodes.

70. (New) The computer system as recited in Claim 64, further comprising instructions to perform the step of addressing the plurality of group controllers using a single virtual address.

71. (New) An apparatus for managing addition and deletion of network nodes from and to a secure multicast or broadcast group of network nodes in a communications network, wherein each of the network nodes is associated with a first group controller comprising information that is replicated in a plurality of group controllers, and wherein the network nodes and the plurality of group controllers are logically organized in a binary tree that represents the network nodes and the plurality of group controllers, in which leaf nodes of the binary tree represent network nodes that are joining or leaving the secure multicast or broadcast group, intermediate nodes represent other network nodes, and root nodes represent the plurality of group controllers, the apparatus comprising:

means for joining the first group controller in a local network in which the plurality of group controllers are coupled;

means for establishing a secure channel between the first group controller and the plurality of group controllers through secure key exchange;

means for receiving a request to add or delete a network node from a load balancer that controls distribution of requests to the plurality of group controllers;

means for generating a new group session key for each network node represented in each branch of the binary tree that is affected by adding or deleting the network node from the secure multicast or broadcast group; and

means for distributing the group session key from the first group controller to the other group controllers of the plurality of group controllers over the secure channel.

72. (New) An apparatus as recited in Claim 71, further comprising means for generating the group session key only when the first group controller is designated as a master group controller that is authorized to join network nodes and generate group session keys.

73. (New) An apparatus as recited in Claim 72, further comprising means for successively designating different group controllers of the plurality of group controllers as the master group controller in real time.

74. (New) An apparatus for creating a secure multicast or broadcast group, the apparatus comprising:

means for establishing a secure communication channel among a plurality of group controllers via a public key exchange protocol;

means for load balancing traffic emanating from a plurality of network nodes to the plurality of group controllers; and

means for distributing a group session key by one of the group controllers based upon a logical arrangement of the network nodes in a binary tree structure, the binary tree structure having a root node, intermediate nodes, and leaf nodes, wherein the plurality of network nodes correspond to leaf nodes of the binary tree structure and the plurality of group controllers correspond to the root node.

75. (New) The apparatus as recited in Claim 74, wherein the means for distributing further comprises:

means for circulating a token among the plurality of group controllers to designate the one group controller as having permission to selectively generate the group session key and keys associated with the intermediate nodes and the leaf nodes; and

means for selectively generating the group session key based upon the circulating step.

76. (New) The apparatus as recited in Claim 74, wherein the means for distributing further comprises:

means for detecting whether the secure multicast or broadcast group has a network node that is leaving the secure multicast or broadcast group;

means for determining which of the intermediate nodes are affected in response to the detecting means;

means for updating keys associated with the affected intermediate nodes;

means for generating a new group session key; and

means for sending the new group session key to the leaf nodes.

77. (New) The apparatus as recited in Claim 76, wherein the means for updating comprises:

means for generating a new key of a parent node of the leaving node; and

means for encrypting the new key of the parent node with a key of a network node adjacent to the parent node.

78. (New) The apparatus as recited in Claim 74, wherein the means for distributing further comprises:

means for receiving a request message from one of the plurality of network nodes to join the secure multicast or broadcast group;

means for determining which of the intermediate nodes are affected in response to the receiving means;

means for updating keys associated with the affected intermediate nodes;

means for generating a new group session key and a private key of the joining node; and

means for sending a message comprising the new group session key, the private key, and the updated keys of affected intermediate nodes to the joining node.

79. (New) The apparatus as recited in Claim 78, wherein the means for updating comprises means for performing a one way hash function on the keys associated with the affected intermediate nodes.

80. (New) The apparatus as recited in Claim 74, further comprising means for addressing the plurality of group controllers using a single virtual address.